

Amendments to the Claims

1 Claim 1 (previously presented): A computer program product embodied on one or more
2 computer-readable media, for establishing a secure connection between a client application and a
3 server application using pre-existing message types, said computer program product comprising:

4 computer-readable program code means for piggy-backing a request for a message
5 encoding scheme proposal onto a first message sent from said client application to said server
6 application, wherein said first message uses a first pre-existing message type;

7 computer-readable program code means for piggy-backing a first portion of security
8 information onto a second message sent from said server application to said client application,
9 wherein said second message uses a second pre-existing message type and wherein said first
10 portion comprises a response to said request for a message encoding scheme;

11 computer-readable program code means for piggy-backing a second portion of security
12 information onto a third message sent from said client application to said server application,
13 wherein said third message uses said first pre-existing message type; and

14 computer-readable program code means for piggy-backing a third portion of security
15 information onto a fourth message sent from said server application to said client application,
16 wherein said fourth message uses a third pre-existing message type.

1 Claim 2 (previously presented): The computer program product according to Claim 1, wherein
2 said first pre-existing message type is a HyperText Transfer Protocol (HTTP) GET request
3 message, said second pre-existing message type is an HTTP REDIRECT message, and said third
4 pre-existing message type is a response to said HTTP GET request message.

Serial No. 09/415,645

-4-

Docket RSW9-99-084

1 Claim 3 (previously presented): The computer program product according to Claim 1, wherein
2 said first pre-existing message type is a HyperText Transfer Protocol (HTTP) POST request
3 message, said second pre-existing message type is an HTTP REDIRECT message, and said third
4 pre-existing message type is a response to said HTTP POST request message.

1 Claim 4 (previously presented): The computer program product according to Claim 1, wherein
2 said first pre-existing message type is a Wireless Session Protocol (WSP) GET request message,
3 said second pre-existing message type is a WSP REDIRECT message, and said third pre-existing
4 message type is a response to said WSP GET request message.

1 Claim 5 (previously presented): The computer program product according to Claim 1, wherein
2 said first pre-existing message type is a Wireless Session Protocol (WSP) POST request message,
3 said second pre-existing message type is a WSP REDIRECT message, and said third pre-existing
4 message type is a response to said WSP POST request message.

1 Claim 6 (original): The computer program product according to Claim 1, wherein:
2 said first message requests a secure page from said server application, wherein said secure
3 page request further comprises an identifier of said secure page;
4 said second message sends a redirection message from said server application to said client
5 application, wherein said redirection message comprises a redirected identifier of said secure page;
6 said third message sends a subsequent request for said secure page from said server

7 application in response to said redirection message, wherein said subsequent request further
8 comprises said redirected identifier of said secure page; and
9 said fourth message sends a response to said subsequent secure page request to said client
10 application, wherein said response further comprises a content portion encrypted using a session
11 key generated by said server application.

1 Claim 7 (original): The computer program product according to Claim 6, wherein:
2 said first portion further comprises a security certificate of said server application;
3 said second portion further comprises a set of information encrypted using a public key of
4 said server application; and
5 said third portion further comprises a nonce of said server application, encrypted using a
6 public key of said client application.

1 Claim 8 (original): The computer program product according to Claim 6, wherein:
2 said first portion further comprises an identification of said server application;
3 said second portion further comprises a set of information encrypted using a public key of
4 said server application; and
5 said third portion further comprises a nonce of said server application, encrypted using a
6 public key of said client application.

1 Claim 9 (original): The computer program product according to Claim 7 or Claim 8, wherein said
2 request for a message encoding scheme further comprises a keyword indicating said request.

1 Claim 10 (original): The computer program product according to Claim 9, wherein said set of
2 information comprises: zero or more parameters required for said secure page request; an
3 identification of said client application; a client nonce; and optionally including a timestamp.

1 Claim 11 (previously presented): The computer program product according to Claim 6, wherein
2 said redirected identifier of said secure page is identical to said identifier of said secure page.

1 Claim 12 (original): The computer program product according to Claim 1, wherein:
2 said first message requests a secure page from said server application, wherein said
3 request further comprises an identifier of said secure page;
4 said second message sends an authentication message from said server application to said
5 client application;
6 said third message sends a subsequent request for said secure page from said server
7 application in response to said authentication message; and
8 said fourth message sends a response to said subsequent secure page request to said client
9 application, wherein said response further comprises a content portion encrypted using a session
10 key generated by said server application.

1 Claim 13 (original): The computer program product according to Claim 12, wherein said
2 authentication message comprises a redirected identifier of said secure page, and wherein said
3 subsequent request further comprises said redirected identifier of said secure page.

1 Claim 14 (previously presented): A system for establishing a secure connection between a client
2 application and a server application using pre-existing message types, said system comprising:

3 means for piggy-backing a request for a message encoding scheme proposal onto a first
4 message sent from said client application to said server application, wherein said first message
5 uses a first pre-existing message type;

6 means for piggy-backing a first portion of security information onto a second message sent
7 from said server application to said client application, wherein said second message uses a second
8 pre-existing message type and wherein said first portion comprises a response to said request for a
9 message encoding scheme;

10 means for piggy-backing a second portion of security information onto a third message
11 sent from said client application to said server application, wherein said third message uses said
12 first pre-existing message type; and

13 means for piggy-backing a third portion of security information onto a fourth message sent
14 from said server application to said client application, wherein said fourth message uses a third
15 pre-existing message type.

1 Claim 15 (previously presented): The system according to Claim 14, wherein said first pre-
2 existing message type is a HyperText Transfer Protocol (HTTP) GET request message, said
3 second pre-existing message type is an HTTP www-Authenticate message header, and said third
4 pre-existing message type is a response to said HTTP GET request message.

1 Claim 16 (previously presented): The system according to Claim 14, wherein said first pre-
2 existing message type is a HyperText Transfer Protocol (HTTP) POST request message, said
3 second pre-existing message type is an HTTP www-Authenticate message header, and said third
4 pre-existing message type is a response to said HTTP POST request message.

1 Claim 17 (previously presented): The system according to Claim 14, wherein said first pre-
2 existing message type is a Wireless Session Protocol (WSP) GET request message, said second
3 pre-existing message type is a WSP www-Authenticate message header, and said third pre-
4 existing message type is a response to said WSP GET request message.

1 Claim 18 (previously presented): The system according to Claim 14, wherein said first pre-
2 existing message type is a Wireless Session Protocol (WSP) POST request message, said second
3 pre-existing message type is a WSP www-Authenticate message header, and said third pre-
4 existing message type is a response to said WSP POST request message.

1 Claim 19 (original): The system according to Claim 14, wherein:
2 said first message requests a secure page from said server application, wherein said
3 request further comprises an identifier of said secure page;
4 said second message sends an authentication message from said server application to said
5 client application;
6 said third message sends a subsequent request for said secure page from said server
7 application in response to said authentication message; and

8 said fourth message sends a response to said subsequent secure page request to said client
9 application, wherein said response further comprises a content portion encrypted using a session
10 key generated by said server application.

1 Claim 20 (original): The system according to Claim 19, wherein said authentication message
2 comprises a redirected identifier of said secure page, and wherein said subsequent request further
3 comprises said redirected identifier of said secure page.

1 Claim 21 (original): The system according to Claim 19 or Claim 20, wherein:
2 said first portion further comprises a security certificate of said server application;
3 said second portion further comprises a set of information encrypted using a public key of
4 said server application; and
5 said third portion further comprises a nonce of said server application, encrypted using a
6 public key of said client application.

1 Claim 22 (original): The system according to Claim 19 or Claim 20, wherein:
2 said first portion further comprises an identification of said server application;
3 said second portion further comprises a set of information encrypted using a public key of
4 said server application; and
5 said third portion further comprises a nonce of said server application, encrypted using a
6 public key of said client application.

1 Claim 23 (original): The system according to Claim 20, wherein said request for a message
2 encoding scheme further comprises a keyword indicating said request.

1 Claim 24 (original): The system according to Claim 23, wherein said set of information
2 comprises: zero or more parameters required for said secure page request; an identification of
3 said client application; a client nonce; and optionally including a timestamp.

1 Claim 25 (original): The system according to Claim 22, wherein said request for a message
2 encoding scheme further comprises a keyword indicating said request and wherein said set of
3 information comprises: zero or more parameters required for said secure page request; an
4 identification of said client application; a client nonce; and optionally including a timestamp.

1 Claim 26 (previously presented): The system according to Claim 20, wherein said redirected
2 identifier of said secure page is identical to said identifier of said secure page.

1 Claim 27 (original): The system according to Claim 14, wherein:
2 said first message requests a secure page from said server application, wherein said
3 request further comprises an identifier of said secure page;
4 said second message sends a redirection message from said server application to said client
5 application, wherein said redirection message comprises a redirected identifier of said secure page;
6 said third message sends a subsequent request for said secure page from said server
7 application in response to said redirection message, wherein said subsequent request further

comprises said redirected identifier of said secure page; and

said fourth message sends a response to said subsequent secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

Claim 28 (previously presented): A method for establishing a secure connection between a client application and a server application using pre-existing message types, said method comprising the steps of:

piggy-backing a request for a message encoding scheme proposal onto a first message sent from said client application to said server application, wherein said first message uses a first pre-existing message type;

piggy-backing a first portion of security information onto a second message sent from said server application to said client application, wherein said second message uses a second pre-existing message type and wherein said first portion comprises a response to said request for a message encoding scheme;

piggy-backing a second portion of security information onto a third message sent from said client application to said server application, wherein said third message uses said first pre-existing message type; and

piggy-backing a third portion of security information onto a fourth message sent from said server application to said client application, wherein said fourth message uses a third pre-existing message type.

1 Claim 29 (previously presented): The method according to Claim 28, wherein said first pre-
2 existing message type is a HyperText Transfer Protocol (HTTP) GET request message, said
3 second pre-existing message type is an HTTP www-Authenticate message header, and said third
4 pre-existing message type is a response to said HTTP GET request message.

1 Claim 30 (previously presented): The method according to Claim 28, wherein said first pre-
2 existing message type is a HyperText Transfer Protocol (HTTP) POST request message, said
3 second pre-existing message type is an HTTP www-Authenticate message header, and said third
4 pre-existing message type is a response to said HTTP POST request message.

1 Claim 31 (previously presented): The method according to Claim 28, wherein said first pre-
2 existing message type is a Wireless Session Protocol (WSP) GET request message, said second
3 pre-existing message type is a WSP www-Authenticate message header, and said third pre-
4 existing message type is a response to said WSP GET request message.

1 Claim 32 (previously presented): The method according to Claim 28, wherein said first pre-
2 existing message type is a Wireless Session Protocol (WSP) POST request message, said second
3 pre-existing message type is a WSP www-Authenticate message header, and said third pre-
4 existing message type is a response to said WSP POST request message.

1 Claim 33 (original): The method according to Claim 28, wherein:
2 said first message requests a secure page from said server application, wherein said

3 request further comprises an identifier of said secure page;

4 said second message sends an authentication message from said server application to said
5 client application;

6 said third message sends a subsequent request for said secure page from said server
7 application in response to said authentication message; and

8 said fourth message sends a response to said subsequent secure page request to said client
9 application, wherein said response further comprises a content portion encrypted using a session
10 key generated by said server application.

1 Claim 34 (original): The method according to Claim 33, wherein said authentication message
2 comprises a redirected identifier of said secure page, and wherein said subsequent request further
3 comprises said redirected identifier of said secure page.

1 Claim 35 (original): The method according to Claim 33 or Claim 34, wherein:

2 said first portion further comprises a security certificate of said server application;

3 said second portion further comprises a set of information encrypted using a public key of
4 said server application; and

5 said third portion further comprises a nonce of said server application, encrypted using a
6 public key of said client application.

1 Claim 36 (original): The method according to Claim 33 or Claim 34, wherein:

2 said first portion further comprises an identification of said server application;

3 said second portion further comprises a set of information encrypted using a public key of
4 said server application; and

5 said third portion further comprises a nonce of said server application, encrypted using a
6 public key of said client application.

1 Claim 37 (original): The method according to Claim 34, wherein said request for a message
2 encoding scheme further comprises a keyword indicating said request.

1 Claim 38 (original): The method according to Claim 37, wherein said set of information
2 comprises: zero or more parameters required for said secure page request; an identification of
3 said client application; a client nonce; and optionally including a timestamp.

1 Claim 39 (original): The method according to Claim 36, wherein said request for a message
2 encoding scheme further comprises a keyword indicating said request and wherein said set of
3 information comprises: zero or more parameters required for said secure page request; an
4 identification of said client application; a client nonce; and optionally including a timestamp.

1 Claim 40 (previously presented): The method according to Claim 34, wherein said redirected
2 identifier of said secure page is identical to said identifier of said secure page.

1 Claim 41 (original): The method according to Claim 28, wherein:
2 said first message requests a secure page from said server application, wherein said

3 request further comprises an identifier of said secure page;

4 said second message sends a redirection message from said server application to said client
5 application, wherein said redirection message comprises a redirected identifier of said secure page;

6 said third message sends a subsequent request for said secure page from said server
7 application in response to said redirection message, wherein said subsequent request further
8 comprises said redirected identifier of said secure page; and

9 said fourth message sends a response to said subsequent secure page request to said client
10 application, wherein said response further comprises a content portion encrypted using a session
11 key generated by said server application.

1 Claim 42 (currently amended): A method for establishing a secure connection between a client
2 application and a server application using pre-existing message types, said method comprising the
3 steps of:

4 piggy-backing a request for said server application to select a message encoding scheme
5 onto a first message sent from said client application to said server application, wherein said first
6 message uses a first pre-existing message type to request content from, or deliver content to, said
7 server application; and

8 piggy-backing a first portion of security information onto a second message sent from said
9 server application to said client application, wherein said second message uses a second pre-
10 existing message type and responds to said first message by sending security-sensitive content,
11 wherein said security-sensitive content is encrypted using a server-application-selected message
12 encoding scheme that is thereby proposed to said client application and said first portion enables

Serial No. 09/415,645

-16-

Docket RSW9-99-084

13 said client application to decrypt said security-sensitive content.

1 Claim 43 (previously presented): The method according to Claim 42, wherein said first pre-
2 existing message type is a HyperText Transfer Protocol (HTTP) GET request message and said
3 second pre-existing message type is a response to said HTTP GET request message.

1 Claim 44 (previously presented): The method according to Claim 42, wherein said first pre-
2 existing message type is a HyperText Transfer Protocol (HTTP) POST request message and said
3 second pre-existing message type is a response to said HTTP POST request message.

1 Claim 45 (previously presented): The method according to Claim 42, wherein said first pre-
2 existing message type is a Wireless Session Protocol (WSP) GET request message and said
3 second pre-existing message type is a response to said WSP GET request message.

1 Claim 46 (previously presented): The method according to Claim 42, wherein said first pre-
2 existing message type is a Wireless Session Protocol (WSP) POST request message and said
3 second pre-existing message type is a response to said WSP POST request message.

1 Claim 47 (currently amended): The method according to Claim 42, wherein:
2 said first message requests ~~a secure page~~ said security-sensitive content from said server
3 application, wherein said request further comprises an identifier ~~[[of]]~~ with which said secure page
4 security-sensitive content can be located; ~~[[and]]~~

Serial No. 09/415,645

-17-

Docket RSW9-99-084

5 ~~said security-sensitive content in said second message sends a response to said secure page~~
6 ~~request to said client application, wherein said response further comprises a content portion is~~
7 ~~encrypted using a session key generated by said server application; and~~
8 said first portion secures said session key while enabling said client application to recover
9 said session key.

1 Claim 48 (currently amended): The method according to Claim 47, wherein:

2 said request to select a message encoding scheme further comprises an identifier of said
3 client application, a nonce of said client application, and optionally ~~including~~ includes a
4 timestamp; and

5 ~~said first portion is secured further comprises a set of information encrypted using a public~~
6 ~~key of said server application.~~

1 Claim 49 (currently amended): The method according to Claim 48, wherein said ~~set of~~
2 ~~information~~ first portion further comprises:

3 a nonce of said server application, encrypted using a public key of said client application;
4 and

5 a security certificate of said server application.

1 Claim 50 (currently amended): The method according to Claim 48 or Claim 49, wherein first
2 message further comprises zero or more parameters required for said server application to use
3 when preparing said secure page request security-sensitive content.

Serial No. 09/415,645

-18-

Docket RSW9-99-084

1 Claim 51 (currently amended): A system for establishing a secure connection between a client
2 application and a server application using pre-existing message types, said system comprising:

3 means for piggy-backing a request for said server application to select a message encoding
4 scheme onto a first message sent from said client application to said server application, wherein
5 said first message uses a first pre-existing message type to request content from, or deliver
6 content to, said server application; and

7 means for piggy-backing a first portion of security information onto a second message sent
8 from said server application to said client application, wherein said second message uses a second
9 pre-existing message type and responds to said first message by sending security-sensitive
10 content, wherein said security-sensitive content is encrypted using a server-application-selected
11 message encoding scheme that is thereby proposed to said client application and said first portion
12 enables said client application to decrypt said security-sensitive content.

1 Claim 52 (previously presented): The system according to Claim 51, wherein said first pre-
2 existing message type is a HyperText Transfer Protocol (HTTP) GET request message and said
3 second pre-existing message type is a response to said HTTP GET request message.

1 Claim 53 (previously presented): The system according to Claim 51, wherein said first pre-
2 existing message type is a Wireless Session Protocol (WSP) GET request message and said
3 second pre-existing message type is a response to said WSP GET request message.

1 Claim 54 (currently amended): The system according to Claim 51, wherein:

2 said first message requests ~~a secure page~~ said security-sensitive content from said server
3 application, wherein said request further comprises an identifier ~~[[of]]~~ with which said ~~secure page~~
4 security-sensitive content can be located; ~~[[and]]~~

5 said security-sensitive content in said second message ~~sends a response to said secure page~~
6 ~~request to said client application, wherein said response further comprises a content portion is~~
7 encrypted using a session key generated by said server application; and

8 said first portion secures said session key while enabling said client application to recover
9 said session key.

1 Claim 55 (currently amended): The system according to Claim 54, wherein:

2 said request to select a message encoding scheme further comprises an identifier of said
3 client application, a nonce of said client application, and optionally ~~including~~ includes a
4 timestamp; and

5 said first portion is secured ~~further comprises a set of information encrypted~~ using a public
6 key of said server application.

1 Claim 56 (currently amended): The system according to Claim 55, wherein said ~~set of~~

2 ~~information~~ first portion further comprises:

3 a nonce of said server application, encrypted using a public key of said client application;

4 and

5 a security certificate of said server application.

Serial No. 09/415,645

-20-

Docket RSW9-99-084

1 Claim 57 (currently amended): The system according to Claim 55 or Claim 56, wherein first
2 message further comprises zero or more parameters required for said server application to use
3 when preparing said secure page request security-sensitive content.

1 Claim 58 (currently amended): A computer program product embodied on one or more
2 computer-readable media, for establishing a secure connection between a client application and a
3 server application using pre-existing message types, said computer program product comprising:

4 computer-readable program code means for piggy-backing a request for said server
5 application to select a message encoding scheme onto a first message sent from said client
6 application to said server application, wherein said first message uses a first pre-existing message
7 type to request content from, or deliver content to, said server application; and

8 computer-readable program code means for piggy-backing a first portion of security
9 information onto a second message sent from said server application to said client application,
10 wherein said second message uses a second pre-existing message type and responds to said first
11 message by sending security-sensitive content, wherein said security-sensitive content is encrypted
12 using a server-application-selected message encoding scheme that is thereby proposed to said
13 client application and said first portion enables said client application to decrypt said security-
14 sensitive content.

1 Claim 59 (previously presented): The computer program product according to Claim 58, wherein
2 said first pre-existing message type is a HyperText Transfer Protocol (HTTP) GET request

3 message and said second pre-existing message type is a response to said HTTP GET request
4 message.

1 Claim 60 (previously presented): The computer program product according to Claim 58, wherein
2 said first pre-existing message type is a Wireless Session Protocol (WSP) GET request message
3 and said second pre-existing message type is a response to said WSP GET request message.

1 Claim 61 (currently amended): The computer program product according to Claim 58, wherein:
2 said first message requests ~~a secure page~~ said security-sensitive content from said server
3 application, wherein said request further comprises an identifier ~~[[of]]~~ with which said ~~secure page~~
4 security-sensitive content can be located; [[and]]
5 ~~said security-sensitive content in said second message sends a response to said secure page~~
6 ~~request to said client application, wherein said response further comprises a content portion is~~
7 ~~encrypted using a session key generated by said server application; and~~
8 said first portion secures said session key while enabling said client application to recover
9 said session key.

1 Claim 62 (currently amended): The computer program product according to Claim 61, wherein:
2 said request to select a message encoding scheme further comprises an identifier of said
3 client application, a nonce of said client application, and optionally ~~including~~ includes a
4 timestamp; and
5 ~~said first portion is secured~~ further comprises ~~a set of information encrypted using a public~~

6 key of said server application.

1 Claim 63 (currently amended): The computer program product according to Claim 62, wherein
2 said set of information first portion further comprises:

3 a nonce of said server application, encrypted using a public key of said client application;

4 and

5 a security certificate of said server application.

1 Claim 64 (currently amended): The computer program product according to Claim 62 or Claim
2 63, wherein first message further comprises zero or more parameters required for said server
3 application to use when preparing said secure page request security-sensitive content.

1 Claim 65 (previously presented): A method for securely establishing a connection between a
2 client application and a server application, further comprising steps of:

3 sending, from the client application to the server application, a first message that uses a
4 first pre-existing message type, wherein the first message requests information from the server
5 application and includes a parameter portion, the parameter portion containing zero or more
6 parameters that may be used by the server application in creating the requested information; and

7 sending, from the server application to the client application, a second message,
8 responsive to receiving the first message, wherein:

9 the second message uses a second pre-existing message type;

10 the second message contains the requested information, which has been created

11 using zero or more of the zero or more parameters and which has been encrypted using a session
12 key;
13 the session key has been created using a server nonce; and
14 the second message further contains the server nonce, encrypted using a public key
15 of the client application.

1 Claim 66 (previously presented): The method according to Claim 65, wherein a client nonce is
2 also used when creating the session key, and wherein the client nonce is transmitted on the first
3 message.

1 Claim 67 (previously presented): A method for securely establishing a connection between a
2 client application and a server application, further comprising steps of:

3 sending, from the client application to the server application, a first message that uses a
4 first pre-existing message type, wherein the first message requests information from the server
5 application and signals the server application to propose an encoding scheme to be used for
6 securely establishing the connection;

7 sending, from the server application to the client application, a second message in
8 response to the first message, wherein the second message uses a second pre-existing message
9 type and requests the client application to re-send the information request from the first message,
10 and wherein the second message also transmits a description of the encoding scheme proposed by
11 the server application;

12 sending, from the client application to the server application, a third message in response

13 to the second message, wherein the third message uses the first pre-existing message type and re-
14 sends the information request from the first message, along with zero or more parameters to be
15 used by the server application in creating the requested information and first security information
16 for use by the server application in securely establishing the connection, according to the
17 described encoding scheme; and

18 sending, from the server application to the client application, a fourth message in response
19 to the third message, wherein the fourth message uses a third pre-existing message type and
20 contains the requested information, which has been encrypted using a session key created using
21 the first security information as an input, and wherein the fourth message further comprises
22 second security information which was also used as an input when creating the session key, the
23 second security information encrypted such that it can be decrypted only by the client application.

1 Claim 68 (previously presented): The method according to Claim 67, wherein the parameters are
2 encrypted using a public key of the server, according to the described encoding scheme.

1 Claim 69 (previously presented): The method according to Claim 67, wherein the first security
2 information comprises a client nonce and the second security information comprises a server
3 nonce.

1 Claim 70 (new): A system for securely establishing a connection between a client application and
2 a server application, comprising:

3 means for sending, from the client application to the server application, a first message

4 that uses a first pre-existing message type, wherein the first message requests information from
5 the server application and includes a parameter portion, the parameter portion containing zero or
6 more parameters that may be used by the server application in creating the requested information;
7 and

8 means for sending, from the server application to the client application, a second message,
9 responsive to receiving the first message, wherein:

10 the second message uses a second pre-existing message type;

11 the second message contains the requested information, which has been created
12 using zero or more of the zero or more parameters and which has been encrypted using a session
13 key;

14 the session key has been created using a server nonce; and

15 the second message further contains the server nonce, encrypted using a public key
16 of the client application.

1 Claim 71 (new): The system according to Claim 70, wherein a client nonce is also used when
2 creating the session key, and wherein the client nonce is transmitted on the first message.

1 Claim 72 (new): A system for securely establishing a connection between a client application
2 and a server application, comprising:

3 means for sending, from the client application to the server application, a first message
4 that uses a first pre-existing message type, wherein the first message requests information from
5 the server application and signals the server application to propose an encoding scheme to be used

6 for securely establishing the connection;

7 means for sending, from the server application to the client application, a second message
8 in response to the first message, wherein the second message uses a second pre-existing message
9 type and requests the client application to re-send the information request from the first message,
10 and wherein the second message also transmits a description of the encoding scheme proposed by
11 the server application;

12 means for sending, from the client application to the server application, a third message in
13 response to the second message, wherein the third message uses the first pre-existing message
14 type and re-sends the information request from the first message, along with zero or more
15 parameters to be used by the server application in creating the requested information and first
16 security information for use by the server application in securely establishing the connection,
17 according to the described encoding scheme; and

18 means for sending, from the server application to the client application, a fourth message
19 in response to the third message, wherein the fourth message uses a third pre-existing message
20 type and contains the requested information, which has been encrypted using a session key
21 created using the first security information as an input, and wherein the fourth message further
22 comprises second security information which was also used as an input when creating the session
23 key, the second security information encrypted such that it can be decrypted only by the client
24 application.

1 Claim 73 (new): The system according to Claim 72, wherein the parameters are encrypted using a
2 public key of the server, according to the described encoding scheme.

1 Claim 74 (new): The system according to Claim 72, wherein the first security information
2 comprises a client nonce and the second security information comprises a server nonce.

1 Claim 75 (new): A computer program product for securely establishing a connection between a
2 client application and a server application, the computer program product embodied on one or
3 more computer-readable media and comprising:

4 computer-readable program code means for sending, from the client application to the
5 server application, a first message that uses a first pre-existing message type, wherein the first
6 message requests information from the server application and includes a parameter portion, the
7 parameter portion containing zero or more parameters that may be used by the server application
8 in creating the requested information; and

9 computer-readable program code means for sending, from the server application to the
10 client application, a second message, responsive to receiving the first message, wherein:

11 the second message uses a second pre-existing message type;

12 the second message contains the requested information, which has been created
13 using zero or more of the zero or more parameters and which has been encrypted using a session
14 key;

15 the session key has been created using a server nonce; and

16 the second message further contains the server nonce, encrypted using a public key
17 of the client application.

1 Claim 76 (new): The computer program product according to Claim 75, wherein a client nonce is
2 also used when creating the session key, and wherein the client nonce is transmitted on the first
3 message.

1 Claim 77 (new): A computer program product for securely establishing a connection between a
2 client application and a server application, the computer program product embodied on one or
3 more computer-readable media and comprising:

4 computer-readable program code means for sending, from the client application to the
5 server application, a first message that uses a first pre-existing message type, wherein the first
6 message requests information from the server application and signals the server application to
7 propose an encoding scheme to be used for securely establishing the connection;

8 computer-readable program code means for sending, from the server application to the
9 client application, a second message in response to the first message, wherein the second message
10 uses a second pre-existing message type and requests the client application to re-send the
11 information request from the first message, and wherein the second message also transmits a
12 description of the encoding scheme proposed by the server application;

13 computer-readable program code means for sending, from the client application to the
14 server application, a third message in response to the second message, wherein the third message
15 uses the first pre-existing message type and re-sends the information request from the first
16 message, along with zero or more parameters to be used by the server application in creating the
17 requested information and first security information for use by the server application in securely
18 establishing the connection, according to the described encoding scheme; and

Serial No. 09/415,645

-29-

Docket RSW9-99-084

19 computer-readable program code means for sending, from the server application to the
20 client application, a fourth message in response to the third message, wherein the fourth message
21 uses a third pre-existing message type and contains the requested information, which has been
22 encrypted using a session key created using the first security information as an input, and wherein
23 the fourth message further comprises second security information which was also used as an input
24 when creating the session key, the second security information encrypted such that it can be
25 decrypted only by the client application.

1 Claim 78 (new): The computer program product according to Claim 77, wherein the parameters
2 are encrypted using a public key of the server, according to the described encoding scheme.

1 Claim 79 (new): The computer program product according to Claim 77, wherein the first security
2 information comprises a client nonce and the second security information comprises a server
3 nonce.